REMARKS

Claims 1-28 were pending in the patent application. The Examiner has rejected Claims 1, 15, 17, 19 and 21 under 35 USC 102(e) as anticipated by Liu; has rejected Claims 1, 2, 5, 7, 15, 17, 19, 21-22, 25 and 27 under 35 USC 102(e) as being anticipated by Godfrey; Claims 7, 10-14 and 22-24 under 35 USC 103(a) as being unpatentable over Liu in view of Gupta; Claims 3-4, 6-9, 16, 26 and 28-29 as being unpatentable over Godfrey in view of Spelman; Claims 18 and 20 as being unpatentable over Boeyen in view of Spelman; and, Claim 8 as unpatentable over Godfrey in view of Owen. For the reasons set forth below, Applicants believe that the claims, as amended, are patentable over the cited art.

The present invention provides a system, method, and computer program means for providing digital signing of communications to be transmitted and for providing verification of digital signatures on communications which have been received. The invention provides the digital signing and signature verification without the need to alter the applications which are generating the communications. Accordingly, the invention provides a proxy server and computer-implemented method at a proxy server whereby a key for creating the digital signature for the communication is

selected based on an analysis of the contents of the message document that is being exchanged by the communication, wherein the contents do not include any digital signature data. Once the key has been selected, the digital signature is created for the message document, after which the message document and its digital signature are transmitted. The application which generated the message document/communication in not involved in the creation of the digital signature and need not, therefore, be modified to provide the functionality. Further, for an incoming communication, the proxy server intercepts the communication, selects a public key for verifying the digital signature based on the contents of the message document in the received communication, verifies the digital signature based on the selected public key, and then allows the communication to go to the destination application. The claims have been amended to further highlight the distinction over the prior art that a key for signing a message is selected from multiple keys, wherein each of said multiple keys is used to sign messages having particular message contents.

The Liu patent is directed to a secure transmission system wherein a message is signed using the private key of the sender and is encrypted using the public key provided by

the recipient (see: Abstract and the key server description found in Col. 19 at lines 57-67). The Liu discussion of the key server 108 does not teach or suggest that the key server determines a digital signature key based on the message contents. Liu teaches that the sender's private key is used to sign all packages from that sender. Clearly, therefore, the Liu patent does not anticipate claim language which expressly recites steps and means for determining a key for digital signature based on message contents, wherein the contents do not include any digital signature data.

The Godfrey patent is directed to a system and method for signing markup language data communicated between first and second units. The signing of the data is done by at least one proxy interposed between the first and second unit. Under Godfrey, the data to be signed includes embedded digital signature initiation data which is detected by the digital signature initiation data detector, 116 of Fig. 1, of the proxy, 108 (see: e.g., Col. 3, lines 34-36 and Col. 4, lines 3-7). The application which generates the markup language data to be signed also generates the digital signature initiation data that tells the proxy to sign the data. Applicants respectfully assert that the Godfrey patent does not anticipate the invention as set forth in amended Claims 7, 10-11 and 22-24. The presently pending

claims expressly recite that a key for creating, or for verifying, a digital signature is selected based on the contents of the message document of the communication, wherein said contents do not include any digital signature data. An analysis of the contents of the message document is done by the proxy in order to select the appropriate key for signing, or for verifying, a communication. The analysis is not simply detection of information embedded by an application when the application generated the communication. In fact, as noted above, the present invention expressly provides for digital signing and signature verification without involvement of the application(s), such that the contents of the message document do not contain any digital signature information.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the neither the Liu nor the Godfrey patent teaches steps or means for creating or verifying a digital signature for a communication/message document, including selecting a key based on the contents of the communication/message document, wherein the contents do not include any digital signature information, and using the key to create or to verify the digital signature, it cannot be maintained that

either Liu or Godfrey anticipates the invention as set forth in the amended claims, Claims 1, 2, 5, 7, 15, 17, 19, 21-22, 25 and 27.

In the ***Response to Arguments*** section, the Examiner states that the argued claim limitations are not recited in Claims 7 and 22. Applicants respectfully assert that those claims, as amended on June 22, 2005, recite that the proxy server intercepts a communication, "provides a digital signature for a message document exchanged via said communication based on the contents of the message document, wherein said contents do not include any digital signature data" (see: Claim 7).

With regard to the rejections under 35 USC 103, Applicants further assert that the claims are patentable over the teachings of the primary references, Godfrey and Liu, in view of the additionally-cited art. In rejecting Claims 7, 10-14 and 22-24, the Examiner has acknowledged that Liu does not explicitly teach a proxy server performing verification. While the newly-cited Gupta reference does provide intermediate stations verifying digital signatures, Gupta does not teach or suggest a proxy server which provides a digital signature for a message document exchanged via said communication based on the contents of

the message document, wherein said contents do not include any digital signature data.

Regarding Claims 3, 4, 6, 9, 16, 26, and 28-29, the Examiner has cited Godfrey but has acknowledged that Godfrey does not provide teachings regarding the replacement key. Accordingly, the Examiner has further cited the Spelman patent in rejecting those claims. The Spelman patent is cited for its teachings related to using a replacement key if a central authority's root key/private key has been compromised. Applicants respectfully assert that the addition of the Spelman patent teachings would not render the present claims unpatentable. Spelman does not provide those teachings which are missing from Godfrey, Boeyen, or the combination of Godfrey and Boeyen. Moreover, Spelman simply provides for the generation of a new key (see: e.g., Col. 4, line 65-Col. 5, line 8), which is neither based on the contents of the data to be communicated nor is it related to the satisfaction of key selection rules set for the key which has been selected based on those contents. Clearly, the addition of the teachings of the Spelman patent to the cited art does not result in the invention as claimed.

In rejecting Claims 18 and 20, the Examiner has cited the Boeyen patent, stating that Boeyen discloses managing a

plurality of private keys to generate a digital signature. The Boeyen patent is directed to an apparatus and method for converting certificates from one format to another format. Under Boeyen, an existing certificate is accompanied by "desired certificate format criteria data" (see: e.g., the Abstract). When the first certificate with desired certificate format criteria data is received at the certificate converting unit, 24 of Fig. 1, the certificate converting unit simply generates a second certificate in the desired format.

Applicants respectfully assert that the addition of the Boeyen patent teachings to Spelman would not result in the invention as claimed. Boeyen requires that the data which is to be processed (i.e., the first certificate) be accompanied by "instruction information", specifically the desired certificate format criteria data. In contrast, the present invention provides for digital signing and digital signature verification based on message document contents, wherein the contents do not include any digital signature information. As discussed above, under the present invention, the application which generates the communication/message document is not aware of the digital signing and does not have to be altered for the inventive method to be implemented.

Applicants further note that the cited Boeyen teachings from Fig. 6 and 7 and Co. 7, lines 11-14 do not teach or suggest the claimed key selection rules. What Boeyen describes is an enable/disable signal which prevents a certificate from being generated in any format, wherein the format (i.e., 212a or 212b) is designated by the desired certificate format criteria data. Boeyen does not teach or suggest selection rules or the use of selection rules for key selection based on message document contents.

In rejecting Claim 8, the Examiner has acknowledged that "Godfrey fails to teach keys to be changed" *(sic)*. Owen is cited for disclosing different sized keys having different security levels. Such is not the same as or suggestive of selecting a key based on message contents and permitting the selected key to be changed in accordance with the message contents. Moreover, the claim expressly recites that the proxy server sets key selection rules for the key and permits digital signature using the key when the selection rules have been satisfied. Clearly the combination of Godfrey and Owen does not teach the invention as claimed.

Since not one of the cited references teaches the claim features, including means and steps for selecting a key based on the contents of the message document, wherein the

contents do not include digital signature information, a *prima facie* case of obviousness simply has not been presented by the Examiner *(In re Wilson,* 424 F.2d 1382, 165 USPQ 494 (C.C.P.A. 1970)). Accordingly, Applicants conclude that Claims 1-2, 5, 8, 17, 19 and 21 are not rendered obvious by the combination of cited references.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

H. Maruyama, et al

By: Anne Vachon Dougherty

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910